UCRL-JC-121099-Abs

A Probabilistic Security Risk Assessment Methodology for Quantification of Public Risk

Douglas Stephens, John A. Futterman, Alfred A. Parziale,
Andrew Randazzo, and Arnold S. Warshawsky

Lawrence Livermore National Laboratory

June 15, 1995

We have developed a methodology that integrates the frequency of deliberate plots, the probability of interdicting such plots, the probability of a successful attack on a nuclear site, and the consequences of nuclear material theft, radiological dispersion or detonation resulting from the attack into an overall probabilistic estimate of risk to the public.

Quantitative probabilistic safety assessments date back to the 1970s, including nuclear accident assessments (both nuclear reactors and weapons). As a result, methodologies have been developed, and there are considerable databases (based on experimental and computational information) for accident frequencies, abnormal environments, and consequences. Thus, the process for quantitative, probabilistic safety assessments of public risk is relatively mature, although improvements continue to be identified and implemented.

Similarly, the state of the art for performing nuclear security assessments is relatively advanced. Both the DOE and DoD have established policies and standards for site security. Each site prepares security plans, carries out self-assessments, and is inspected to ensure compliance with performance criteria. Verification is estimated using vulnerability and conflict simulation codes such as SEES (Security Exercise Evaluation System) or ASSESS. Force-on-force exercises are carried out in many cases.

However, most security or vulnerability assessments begin with the probability of a security attempt and/or attack set to 1.0. Conditional probabilities for successful adverse action are then computed. Thus, estimates of public risk are not obtained.

Yet a direct comparison of security and safety of nuclear sites is needed to understand the relative risks so scarce resources can be allocated in an optimum manner to reduce overall public risks. Further, the interdependence of safety and security can be quantified, i.e., an increase in safety may actually lead to a decrease in security, and vice versa.

Quantitative security/use control assessments enable determination of the relative values of risk reduction measures, including:

- protective force levels, arms and tactics
- physical barriers and sensors
- counterterrorism intelligence information gathering and analysis capabilities
- passive and active protective features

Given an attack, the effectiveness in preventing nuclear material theft, deliberate radiological release or detonation is a result of the interaction of numerous factors: facility design, equipment, sensors, defender manpower, training, arms, tactics, and training; and threat: the attacker's tactics, training, arms, equipment, goals, and time, etc. All of these factors are subject to analysis using combat simulation models.

If the estimated risks are acceptable, risk reduction measures are unnecessary. However, if risk reduction is judged to be required, the more cost-effective options need to be identified. These options can be technical or equipment-related, physical, procedural, or administrative.

Detailed cost-benefit calculations can be conducted to rank-order the more cost/beneficial options. Costs include R&D to establish technical feasibility of the option, costs to implement the option, including manufacture if equipment-related, and impacts on operations or safety. Benefits generally result from avoided incident costs: the costs of an incident multiplied by the lifetime probabilities of the incidents. Combined with decision analysis, decisions can be made which optimize public surety (safety and security) with the limited resources available including funds, personnel, and other constraints.

*This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract No. W-7405-Eng-48.